

## Vocola MS-1 Voice-over-IP Interface

The Biamp Vocola Message Server (MS-1) includes a feature which allows pages to be initiated over any VoIP system that adheres to the SIP (Session Initiation Protocol) standard. This document details the steps required to configure a Cisco CallManager VoIP system to work with the Biamp Vocola MS-1. The steps below were written based on CallManager version 8.5.1.10000-26, however the configuration of other versions of CallManager should be similar or identical.

## Media Resource Group

The first step to setting up the CallManager system is to create a Media Resource Group and a Media Resource Group List. The instructions below describe the required settings. Throughout this document, any settings which are not mentioned can be left at their default values.

1. Go to Media Resources—>Media Resource Group.
2. Click the "Add New" button.
3. Enter a name and description for the new Media Resource Group. (see Figure 1)
4. Add "MTP\_2" to the Selected Media Resources field by selecting it in the Available Media Resources field and clicking on the down arrow.
5. Click the "Save" button.
6. Go to Media Resources—>Media Resource Group List.
7. Click the "Add New" button.
8. Enter a name for the new Media Resource Group List. (see Figure 2)
9. Select the name of the previously created Media Resource Group (see step 3 above) in the Available Media Resource Groups field, and click the down arrow to move it into the Selected Media Resource Groups field.
10. Click the "Save" button.

**Media Resource Group Information**

Name\*

Description

**Devices for this Group**

Available Media Resources\*\*

Selected Media Resources\*

☐ Use Multicast for MOH Audio (If at least one multicast MOH resource is available)

**Figure 1** – Media Resource Group screen

**Media Resource Group List Information**

Name\*

**Media Resource Groups for this List**

Available Media Resource Groups

Selected Media Resource Groups

**Figure 2** – Media Resource Group List screen

## A Note About System Security

VoIP systems can offer additional security by enabling Digest Authentication. If Digest Authentication is enabled, the Vicia MS-1 will require an encrypted password be sent when a call is being setup. If the passwords between Call Manager and the MS-1 match the call will move forward, if they do not the call will be denied. Digest Authentication is not required by the MS-1 and its use should be determined by the security requirements of the VoIP network. This Tech Note outlines the steps that need to be taken for both circumstances, however the system will only be configured for one option or the other. Digest Authentication steps are valid for this page only, all steps on the following pages should be preformed whether Authentication is used or not.

## Setup For Systems **NOT** Using Digest Authentication

### Security Profile

Next, a new SIP Trunk Security Profile must be created.

1. Go to System—>Security Profile—>SIP Trunk Security Profile.
2. Click the "Add New" button.
3. Enter a name and a description for the new SIP Trunk Security Profile. (see Figure 3)
4. Set the Security Mode to Non Secure.
5. Set the Outgoing Transport Type to UDP.
6. Click the "Save" button.

**SIP Trunk Security Profile Information**

Name *	Biamp Vicia Security Profile
Description	MS-1 VoIP Trunk
Device Security Mode	Non Secure
Incoming Transport Type *	TCP+UDP
Outgoing Transport Type	UDP

**Figure 3** – SIP Trunk Security Profile Screen No Digest Authentication

## Setup For Systems Using Digest Authentication

### Security Profile

Next, a new SIP Trunk Security Profile must be created.

1. Go to System—>Security Profile—>SIP Trunk Security Profile.
2. Click the "Add New" button.
3. Enter a name and a description for the new SIP Trunk Security Profile. (see Figure 4)
4. Set the Security Mode to Non Secure.
5. Set the Outgoing Transport Type to UDP.
6. Check the Box for Enable Digest Authentication.
7. Click the "Save" button.

**SIP Trunk Security Profile Information**

Name *	Biamp Vicia Security DA Profile
Description	MS-1 VoIP Trunk
Device Security Mode	Non Secure
Incoming Transport Type *	TCP+UDP
Outgoing Transport Type	UDP
<input checked="" type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins) *	600
X.509 Subject Name	
Incoming Port *	5060
<input type="checkbox"/> Enable Application Level Authorization	
<input type="checkbox"/> Accept Presence Subscription	
<input type="checkbox"/> Accept Out-of-Dialog REFER **	
<input type="checkbox"/> Accept Unsolicited Notification	
<input type="checkbox"/> Accept Replaces Header	
<input type="checkbox"/> Transmit Security Status	

**Figure 4** – SIP Trunk Security Profile Screen With Digest Authentication

### SIP Realm

A SIP Realm, User, & Password are required for Digest Authentication.

1. Go to User Management —>SIP Realm
2. Enter "vicia" in the Realm Field. Note the Realm is set by the Vicia MS-1 and must be typed exactly in Call Manager. The text must also be lower case. (See Figure 5)
3. Enter "anonymous" in the User Field. This is the Call Manager Default user and it must be matched precisely. (See Figure 5)
4. Enter a password in the Digest Credentials field.
5. Confirm the password.
6. Click the "Save" button.

**SIP Realm Information**

Realm *	vicia
User *	anonymous
Digest Credentials *	.....
Confirm Digest Credentials *	.....

**Figure 5** – SIP Realm Screen With Digest Authentication

## Trunk

The next step is to create a new trunk using the previously created Security Profile.

1. Go to Device—>Trunk.
2. Click the "Add New" button.
3. Set the Trunk Type to SIP Trunk.
4. Set the Device Protocol to SIP.
5. Click the "Next" button.
6. Assign a name and description to the new SIP Trunk. Note that the name cannot include spaces. (see Figure 6)
7. Set the Device Pool to Default.
8. Set the Media Resource Group List to the Media Resource Group List created previously. (see step 8 under Media Resource Group on page 1)
9. Click to select the checkbox for Media Termination Point Required.
10. In the SIP Information section, the Destination Address field must be set to the VoIP IP address of the MS-1.
11. For the SIP Trunk Security Profile, select the Security Profile created earlier. (See Step 3 under Security Profile settings on Page 2)
12. Set the SIP Profile to Standard SIP Profile.
13. Set the DTFM Signaling Method to OOB and RFC2833.
14. Click the "Save" button.

Note that Call Manager may indicate a reset is needed. A reset will be preformed at the end of this Tech Note.

Device Information	
Product:	SIP Trunk
Device Protocol:	SIP
Device Name *	VociaTrunk
Description	MS-1 VoIP Trunk
Device Pool *	Default
Common Device Configuration	< None >
Call Classification *	Use System Default
Media Resource Group List	Biamp Vocia MRGL
Location *	Hub_None
AAR Group	< None >
Packet Capture Mode *	None
Packet Capture Duration	0
<input checked="" type="checkbox"/> Media Termination Point Required <input checked="" type="checkbox"/> Retry Video Call as Audio <input type="checkbox"/> Transmit UTF-8 for Calling Party Name <input type="checkbox"/> Unattended Port	

SIP Information	
Destination Address *	172.16.1.10
<input type="checkbox"/> Destination Address is an SRV	
Destination Port *	5060
MTP Preferred Originating Codec *	711ulaw
Presence Group *	Standard Presence group
SIP Trunk Security Profile *	Biamp Vocia Security Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile *	Standard SIP Profile
DTMF Signaling Method *	OOB and RFC 2833

**Figure 6** – Trunk Configuration screen (some sections omitted)

## Route Pattern

Finally, we need to set up a Route Pattern to define the extension at which the MS-1 will reside.

1. Go to Call Routing—>Route/Hunt—>Route Pattern.
2. Click the "Add New" button.
3. Set the Route Pattern to an extension number that the MS-1 will use. (See Figure 7)
4. Set the Gateway Route List to the previously created Trunk. (See Step 6 under Trunk, Page 3)
5. Set the Route Option to Route This Pattern.
6. Uncheck the checkbox for Provide Outside Dial Tone.
7. Set Calling Line ID Presentation to Restricted.
8. Set Calling Name Presentation to Restricted.
9. Click Save.

### Note

The Voca MS-1 supports multiple extensions to be used on a single Trunk line. A minimum of 1 extension must be assigned for the tie to paging. More extensions can be assigned to facilitate direct page extensions. If this feature is desired repeat Steps 1—9 for each extension to be used.

Note that Call Manager may indicate a reset is needed. A reset will be preformed at the end of this Tech Note.

## Reboot CallManager

Once CallManager has been configured, the VoIP server will either need to be rebooted or the CallManager service will need to be restarted from the CallManager Unified Serviceability Control Center before the changes will take effect.

Pattern Definition	
Route Pattern*	1234
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
Gateway/Route List*	VociaTrunk <a href="#">(Edit)</a>
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error
Call Classification*	OnNet
<input type="checkbox"/> Allow Device Override <input type="checkbox"/> Provide Outside Dial Tone <input type="checkbox"/> Allow Overlap Sending <input type="checkbox"/> Urgent Priority	
<input type="checkbox"/> Require Forced Authorization Code	
Authorization Level*	0
<input type="checkbox"/> Require Client Matter Code	
Calling Party Transformations	
<input type="checkbox"/> Use Calling Party's External Phone Number Mask	
Calling Party Transform Mask	
Prefix Digits (Outgoing Calls)	
Calling Line ID Presentation*	Restricted
Calling Name Presentation*	Restricted

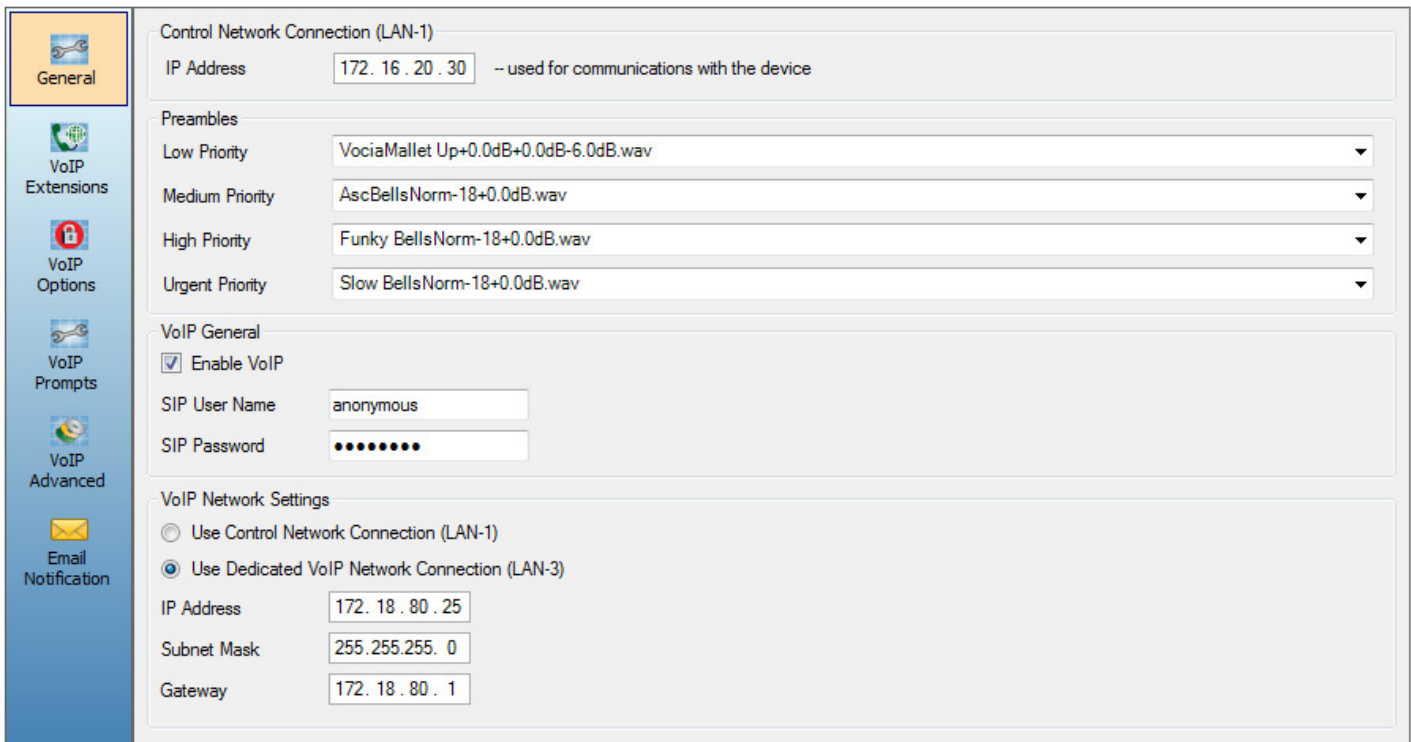
**Figure 7** – Route Pattern Configuration screen (some sections omitted)

## MS-1 Setup

### General Tab Settings

After completing the configuration of the CallManager server, several options in the MS-1 will need to be set to match the CallManager settings.

1. In the Vicia software, open the MS-1 dialog.
2. In the General tab, check the checkbox for "VoIP Enabled".
3. Check the checkbox for "Use Dedicated VoIP Network Connection (LAN 3)".
4. Enter the IP Address for the MS-1 VoIP Port. **The IP address entered here must match the IP address entered into CallManager.** (See Step 10 of the Trunk section on Page 3)
5. Enter an appropriate Subnet Mask & Gateway. If you're not sure what this should be, contact the VoIP system administrator.
6. Set the SIP User Name field to "anonymous". This is the default user name for CallManager, it cannot be changed.
7. If Digest Authentication was used in CallManager (see Page 2) enter the password used in CallManager in the SIP Password field. If Digest Authentication was not used simply enter a dummy password in the SIP Password field. The MS-1 requires that this field be populated, even if a password is not required.
8. Click Save.



**General**

Control Network Connection (LAN-1)

IP Address: 172.16.20.30 -- used for communications with the device

Preambles

Low Priority: VociaMallet Up+0.0dB+0.0dB-6.0dB.wav

Medium Priority: AscBellsNorm-18+0.0dB.wav

High Priority: Funky BellsNorm-18+0.0dB.wav

Urgent Priority: Slow BellsNorm-18+0.0dB.wav

VoIP General

☒ Enable VoIP

SIP User Name: anonymous

SIP Password: ••••••••

VoIP Network Settings

☐ Use Control Network Connection (LAN-1)

☒ Use Dedicated VoIP Network Connection (LAN-3)

IP Address: 172.18.80.25

Subnet Mask: 255.255.255.0

Gateway: 172.18.80.1

**Figure 8** – MS-1 VoIP General Tab in Vicia Software

## MS-1 Setup

### VoIP Extensions Tab Setup

Extension mapping is required in the MS-1. A minimum of 1 extension must be setup in the MS-1 for proper operation. Additional extensions can be added to map extensions to specific page codes. For more information of the setup of individual MS-1 extensions reference the Vocola Help File or contact Biamp Applications Engineering.

1. Select the VoIP Extensions tab.
2. Enter an extension number in the Extension Field. **This number must match the Route Pattern entered into CallManager.** (See Step 3 of the Route Pattern section on Page 4).
3. Enter additional extensions as required.
4. Note that the MS-1 VoIP paging feature supports the use of PIN groups. To enable this, first create the PIN Group(s) in the Universe Properties window, and then select the appropriate PIN Group(s) in the VoIP Options tab of the MS-1.
5. Click Save.

Extensions <span>New</span> <span>Delete</span> <span>Duplicate</span> <span>Extension Wizard</span>											
Ext...	Mapped Page Code	Paging Mode	Ring Count	Pin Access	Welcome	Page Now	Page Recorded	Hang Up	Continuous	Conference	
1000	None	N/A	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2000	002 - Engineering Dept.	Live	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3300	004 - Support Dept.	Live	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9100	013 - Building is Closing	Pre-Recorded	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

**Figure 9** – MS-1 VoIP Extensions Tab in Vocola Software

## MS-1 Setup

### VoIP Advanced Tab Setup

This section of the Tech Note describes the security settings that need to be set. The settings listed here are dependant on whether Digest Authentication was enabled in CallManager (See Page 2). All other settings are normally left at default.

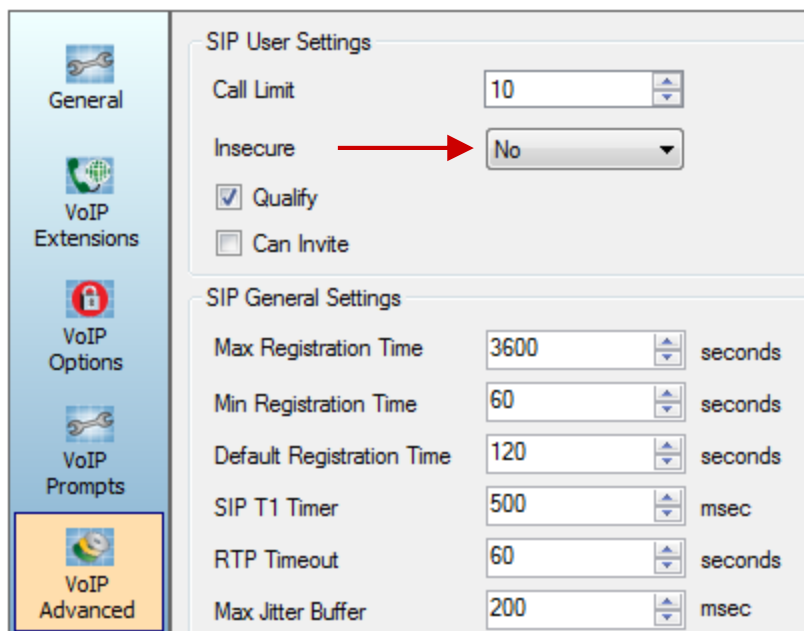
#### Setting if Digest Authentication is ENABLED in CallManager.

Setting if Digest Authentication is **ENABLED** in CallManager.

1. Select the VoIP Advanced tab.
2. Set the Insecure pull down menu to No.
3. Click Save.

#### **Note:**

The Voca Configuration must be loaded to the MS-1 in order for changes to take effect.



**Figure 10** – MS-1 VoIP Advanced Tab in Voca Software

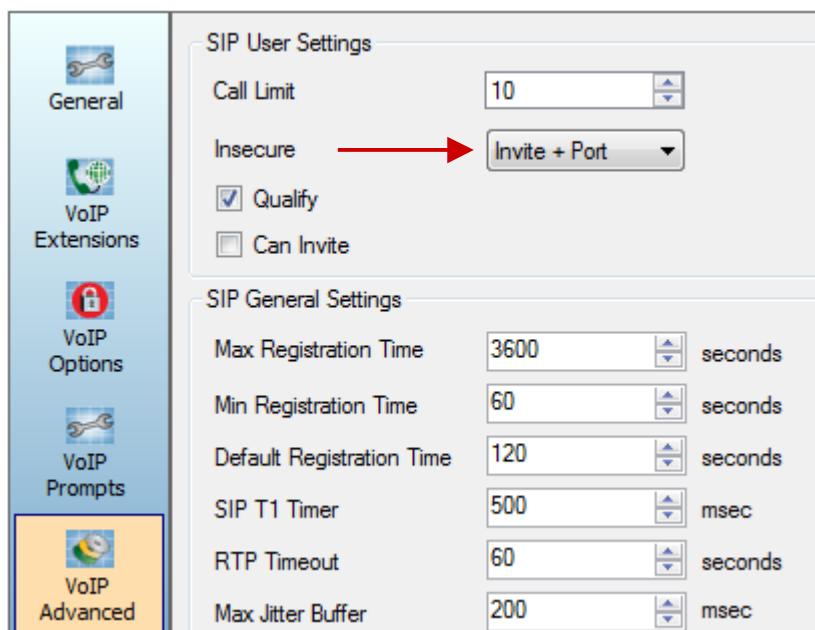
#### Setting if Digest Authentication is NOT enabled in CallManager.

Setting if Digest Authentication is **ENABLED** in CallManager.

1. Select the VoIP Advanced tab.
2. Set the Insecure pull down menu to Invite + Port.
3. Click Save.

#### **Note:**

The Voca Configuration must be loaded to the MS-1 in order for changes to take effect.



**Figure 11** – MS-1 VoIP Advanced Tab in Voca Software